REMARKS

Applicant respectfully requests that the above-identified patent application be reexamined and reconsidered. Claims 1-21 are now pending in this application. In an Office Action dated October 27, 2005 (hereinafter the "Office Action"), Claims 1, 5, 8, 9, 11, 13, 17, 19, and 21 were rejected under 35 U.S.C. § 102(e) as being unpatentable over U.S. Patent No. 6,041,357, issued to Kunzelman et al. (hereinafter "Kunzelman"). Claims 6 and 7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kunzelman further in view of U.S. Patent No. 6,005,853, issued to Wang et al. (hereinafter "Wang"). Claims 2-4, 10, and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kunzelman further in view of U.S. Patent No. 5,999,711, issued to Misra et al. (hereinafter "Misra"). Claims 14-16, 18, and 20 were rejected under 35 U.S.C. § 103(a) in view of Kunzelman, Misra, and further in view of U.S. Patent No. 5,481,539, issued to Hershey et al. (hereinafter "Hershey").

Prior to discussing in detail why applicant believes that all of the claims in the application are allowable, a brief description of applicant's invention and the cited references is provided. The following discussions of the disclosed embodiments of applicant's invention and the teachings of the applied references are not provided to define the scope or interpretation of any of applicant's claims. Instead, such discussed differences are provided to help the U.S. Patent and Trademark Office (hereinafter "the Office") better appreciate important claim distinctions discussed thereafter.

Summary of the Present Invention

The present invention allows users of a client computer to access a second server-based application based on previously provided authorization to access a first server-based application. The access to the second server-based application is based on the previously provided access to a

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

first server-based application that can securely authenticate a client computer without requiring a user to endure a lengthy log-in procedure.

The invention is ideally suited for use with client computers capable of concurrently executing multiple client application programs, such as an instant messaging client application and a Web browser client application. The client computer may make requests to server-based applications. If the client computer is authorized to access a first server-based application, an authorization ticket will be transmitted to the client computer. The authorization ticket includes encrypted data, such as a time stamp indicating the time at which the authentication ticket was created. Once the client computer has been provided authorization to access the first server-based application, a client application starts an elapsed time counter.

In one embodiment of the present invention, when a request is made by the client computer to access a second server-based application, the client application communicating with the first server-based application determines the session length based upon the elapsed time counter. The client application then concatenates the original authorization ticket, the session length, and a secret shared with the second server-based application. A hash function is then applied to the concatenated data to create a unique hash value. The client stores the authorization ticket, the session length, and the hash value in a file that is accessible to a second client application executing on the client computer. The client also starts a persistence timer when the file is saved. The persistence timer is periodically checked to determine if a predetermined amount of time has elapsed. If the predetermined amount of time has elapsed, the file is deleted from the client computer.

The client computer then launches the second client application and causes a log-in request to be transmitted from the second client application to the second server-based application. The request includes the file containing the authorization ticket, the session length,

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

and the hash. The second client application then receives and displays results received from the second server-based application. When the second server-based application receives the request, the authorization ticket is decrypted and the shared secret is obtained from a database. The second server-based application then compares the computed hash value to the hash value received from the second client application. If the two hash values are identical, the second server-based application authorizes the client computer. As a result, a user does not experience multiple log-in procedures when accessing multiple server-based applications.

Summary of Kunzelman

Kunzelman is purportedly directed at an improved session control method in which a client computer establishes a session with a server computer such that the server computer can identify the client computer or a user associated with the client computer. Then, when the client computer wishes to obtain resources that are stored on another server computer, the client requests a session token from the first server computer. The session token is passed from the client computer to the server computer that stores the desired resources.

Summary of Misra

Misra is purportedly directed to a system that has a facility to check authorization and authentication information in a distributed environment. The system includes a principal, such as a portable computer that holds a secure package which may be encrypted or may include a digital signature. Once the principal has been provided with the secure package, the principal may send a request to log in to the distributed system along with authorization and authentication information. The secure package is accessed to determine whether the principal is authorized to connect to the distributed system. Where the principal is not authorized to connect to the distributed system, the principal's request to log in is denied. In contrast, where the principal is authorized to connect to the distributed system, the principal's request to connect is granted.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Summary of Wang

Wang is purportedly directed to a channel access protocol for implementing a wireless data network. More specifically, Wang discloses a network protocol for a high channel utilization. The resulting network access scheme allows a transmitter to send messages to a cellular base station, simultaneously with other transmitters, without the need for retransmission, if the message reaches the receiver with sufficient strength. Multiple transmitters and receivers are distributed over a geographical area, sharing the same frequency channels. As a result, multiple messages are able to capture multiple receivers simultaneously, thereby improving the channel utilization. A message received by a base station is forwarded, either by a wired link or wireless link, to a network control center for routing. The base stations are distributed over a service area in accordance with the expected density of the wireless terminals and the physical attributes of the terrain.

Summary of Hershey

Hershey is purportedly directed to a system for communicating between mobile telephone devices. More specifically, Hershey purportedly discloses a communication protocol where a mobile unit creates a message packet that it desires to transmit to an intended receiver having a unique identification number, such as a mobile telephone number. The initiating mobile unit broadcasts the message packet in low power to local mobile units in the reception area. Each mobile unit that receives the message without errors responds with an acknowledgement signal. Each mobile unit that receives the broadcast determines if the message packet is valid. The mobile units compare the mobile unit identification number of the valid message packets with its own internal identification number. If the identification numbers match, the message was successfully transmitted to the intended mobile unit.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Rejection of Claims 1, 5, 8, 9, 11, 13, 17, 19, and 21 Under 35 U.S.C. § 102(e)

The Office Action rejected Claims 1, 5, 8, 9, 11, 13, 17, 19, and 21 under 35 U.S.C. § 102(e) as being anticipated by Kunzelman. The Office Action asserts that Kunzelman suggests each and every element of Claims 1, 5, 8, 9, 11, 13, 17, 19, and 21. Applicant respectfully disagrees.

Claim 1

As amended, Claim 1 recites:

> A computer-implemented method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application that provides a different service than said second server-based application, comprising:
>
> (a) receiving a request to access the service provided by said second server-based application wherein the service provided by said second server-based application is different than the service provided by said first server-based application;
>
> (b) in response to said request:
>
> (i) determining a session length indicating a length of time said client computer has been authorized to access the service provided by said first server-based application;
>
> (ii) calculating a hash value for an authorization ticket received from said first server-based application, said session length, and a secret shared between said client computer and said second server-based application, and
>
> (iii) transmitting a request for authorization to access the service provided by said second server-based application comprising said hash value, said authorization ticket, and said session length.

Claim 1 of the present invention defines a computer-implemented method for authorizing a client computer to access a server-based application based on a previously provided authorization. More specifically, providing the authorization as recited in Claim 1 includes "receiving a request to access the service provided by said second server-based application **wherein the service provided by said second server-based application is different then the**

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

service provided by said first server-based application." [Emphasis added.] Stated differently, once a client computer is authorized to access a first server-based application, a request to access the services provided by a second server-based application may also be authorized without requiring any additional effort on the part of the user. A user associated with the client computer does not have to endure a second log-in procedure when making a request to access the services provided by the second server-based application. Conversely, Kunzelman is directed at allowing a client computer to access resources, such as Web pages, that are stored on more than one server computer so that a user does not need to know that the resources accessed are on different computers.

The Office Action asserts that Kunzelman teaches authorizing a client computer to access a second server-based application "wherein the service provided by said second server-based application is different then the service provided by said first server-based application," and cites Col. 3, lines 34-44, of Kunzelman in support of that proposition. The relevant portion of Kunzelman states:

> An example of session migration will now be described with reference to a migration of client from a server A to a server B, which might be client 12, server 14A (source server node) and server 14B (target server node). The session migration process begins when client 12 takes action which is to result in a session migration. The session migration moves the client's interaction from channel 20A to channel 20B in a way that is transparent to the client's user, but that also maintains any necessary state, including state variables which indicate a level of authorization for the client's use of the session.

(Kunzelman at Col. 3, lines 34-44.)

The cited portions of Kunzelman do not disclose authorizing a client computer to access a server-based application that provides a different service than a previously accessed server-based application. Moreover, applicant is unable to find any reference in Kunzelman to accessing services provided by multiple applications based on a previous authorization. Instead, the cited

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

portions of Kunzelman describe a process where a client's interactions are migrated "from a server A to a server B," and do not disclose providing access to services of different applications programs. In contrast to the present invention, the cited portions of Kunzelman describe allowing a user to access resources that are stored on different server computers (e.g., server A and server B) by establishing a session on a first server.

Kunzelman is directed at allowing a user to access resources that are stored on different server computers using a single application program, namely a Web server application. In describing the problem solved, Kunzelman states:

> what made the World Wide Web more interesting and complex is the fact that a link in a first document stored on a first server might refer to a document on a second server where the author of the first document and the system operator of the first server had no editorial or system control over the second document or the second server.

(Kunzelman, Col. 1, lines 27-33.)

In the purported description of the solution to the above-described problem, Kunzelman further states that to allow access to resources on a second server:

> [A] client establishes a session with the first server such that the first server can identify the client. When the client wishes to migrate from the first server to a second server, the client requests a session token from the first server.

(Kunzelman at Col. 1, lines 27-33.) The "migration" as disclosed in Kunzelman is defined as providing access to a Web page that is stored on a second server computer. For example, as stated in Kunzelman, a migration between server computers occurs when:

> [A]n operator of a Web server wants to out source the operation of a particular aspect of their Web site. For example, a newspaper might operate a site which provides news, features, and classifieds, but will outsource the management of the classifieds to another operator, such as Electric Classifieds, Inc., of San Francisco, Calif. (the assignee of the present application). A migration occurs when a user selects a classifieds "button" or selection on a Web page operated by the newspaper. The URL

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

> associated with the button can either be a direct reference to the target server or a reference which causes redirection. In the former case, the page containing the button is presented to the user with the underlying HTML anchor including a session token for use in migration. This is possible where the source server can anticipate that a migration may occur. In the latter case, the server need not anticipate the migration in the anchor for the button will be a URL directed at the source server. The source server responds to the URL with a redirection URL. The redirection URL would be the equivalent to the embedded URL with a session token in the former case.

(Kunzelman at Col. 3, lines 45-65.)

A migration as disclosed in Kunzelman merely involves providing access to resources stored on different server computers using a single server-based application program, namely a Web server application program. As the above-cited sections of Kunzelman state, a migration occurs when a user selects an embedded control, such as a "classifieds button," that is presented on a Web page accessed from first server computer. When the embedded control is selected, either a direct Uniform Resource Locator ("URL") or a redirected URL is used to identify the new resource (e.g., Web page) available from the second server computer. Those skilled in the art and others will recognize that a URL identifies a network address in which a particular Web page may be accessed using a client based Web browser application. The URL merely allows access to Web pages by instructing a browser program that executes on a client computer to transmit a request for a Web page using a URL to identify a network address. In response, the user's browser program receives markup code and displays the Web page which, typically, includes various hyperlinks that point to or link other network addresses of other Web pages.

By contrast, the present invention authorizes users to access multiple server-based applications (e.g., a Web server application, instant messaging server application, and the like) without having to be re-authenticated when logic or resources from another server-based application is accessed. For example, a user of the present invention may open an account from a single provider that offers multiple services. In this regard, the user may attempt to access a

restricted Web page from a Web server associated with the provider that requires authentication. After being authenticated, the user may access the Web page. However, based on this previous authentication to the Web server application, the user may also access another application program, for example, that allows instant messaging with another user. In this regard, a server-based instant messaging application associated with the provider may obtain the user's authentication rights from the Web server application. This functionality is described in the present application as follows:

> According to an embodiment of the present invention, a user of the client computer may select a user interface option provided by the instant messaging client application program 12 for gaining quick access to the Web server computer. For instance, a user of the MSN Messenger client application may desire to quickly gain access to their Web-based e-mail account with the HotMail service, also from Microsoft®. In order to provide this functionality, the instant messaging client application program 12 may provide a menu item, button, or other user interface item for quickly accessing the Web server computer 26. In response to the selection of this user interface item, the client computer 10 may gain authorization to access to the Web server computer 26 based upon the previously provided authorization to access the instant messaging server computer 2.

(Present application at page 7.)

Simply stated, authorizing a client computer to access multiple server-based application programs as recited in Claim 1 of the present invention, is not equivalent to allowing a user to migrate between resources stored on different server-based computers as disclosed in Kunzelman. More specifically, Claim 1 of the present invention recites a method for authorizing a client computer "to access the service provided by said second server-based application wherein the service provided by said second server-based application is different then the service provided by said first server-based application." Kunzelman does not disclose a system for allowing access to multiple server-based application programs that provide different types of

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

services. Instead, Kunzelman is limited to providing access to resources on different server computers using a single server-based application program, namely a Web server application program.

For at least the above-mentioned reasons, applicant respectfully submits that the Office Action has not established a *prima facie* case for a Section 102(e) rejection of Claim 1, and respectfully requests that the rejection of Claim 1 and the claims dependent thereon be withdrawn and these claims allowed.

Claim 13

Claim 13 recites:

> A computer-implemented method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application that provides a different service than said second server-based application, comprising:
>
> (a) receiving a request for authorization to access the service provided by said second server-based application from said client computer comprising a hash value, an authorization ticket, and a session length wherein the service provided by said second server-based application is different than the service provided by said first server-based application;
>
> (b) computing a new hash value for said authorization ticket, said session length, and a copy of a secret shared between said client computer and said second server-based application;
>
> (c) determining whether said hash value received from said client computer is identical to said new hash value; and
>
> (d) in response to determining that said hash value received from said client computer is identical to said new hash value, authorizing said client computer to access the service provided by said second server-based application.

Claim 13 of the present invention recites a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. More specifically, the claimed method recites (a) receiving a

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

request for authorization to access said second server-based application from said client computer comprising a hash value, an authorization ticket, and a session length, (b) computing a new hash value for said authorization ticket, said session length and a copy of a secret shared between said client computer and said second server-based application, and (c) in response to determining that said hash value received from said client computer is identical to said new hash value, authorizing said client computer to access said second server-based application.

As described previously with regard to Claim 1, Kunzelman does not disclose a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. Instead, Kunzelman purportedly discloses a system of providing access to resources stored on different server computers through a single server-based application program, namely a Web server application program. Conversely, the present invention authenticates users to access multiple server-based applications. Thus, the present invention is not limited to authorizing a user to accessing resources only available from a single application. Consequently, Kunzelman does not disclose the elements as recited in Claim 13, and applicant respectfully submits that the rejection of Claim 13 is in error and requests that the rejection be withdrawn.

Claims 5, 8, 9, 11, 17, 19, and 21

Since, Claims 5 and 8 depend, directly or indirectly, from Claim 1, and Claims 9 and 11 are computer apparatus and computer-readable medium claims that depend from Claim 1, the analysis applied to Claim 1 also applies to these claims. Also, since Claim 21 depends from Claim 13, and Claims 17 and 19 are computer-controlled apparatus and computer-readable medium claims that depend from Claim 13, the analysis applied to Claim 13 also applies to these claims. Therefore, applicant respectfully submits that Claims 5, 8, 9, 11, 17, 19, and 21 are in condition for allowance for the same reasons as Claims 1 and 13, respectively. In addition,

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

applicant submits that the dependent claims are allowable for additional reasons described below.

Dependent Claim 5 adds to the nonobviousness of applicant's invention of "performing an MD5 hash of an authorization ticket received from said first server-based application, said session length, and a secret shared between said client computer and said second server-based application." The Office Action asserts that Kunzelman teaches performing an MD5 hash of an authorization ticket that includes a session length and a shared secret and references Col. 7, lines 15-27 of Kunzelman in support of that proposition. The referenced section of Kunzelman states that: "Encryption is done using a public key cryptosystem supplied by RSA Data Security, of Palo Alto, Calif., or similar cryptosystem." (Kunzelman at Col. 7, lines 25-27.) The Office Action states that performing in an MD5 is inherent in the cryptosystem supplied by RSA data security. (Office Action at page 4.) The basis of this assertion is not known as applicant is unable to find any reference in Kunzelman to performing an MD5 hash on a set of data that is transmitted between computers. Moreover, Kunzelman does not disclose the additional elements recited in Claim 5 namely performing an MD5 hash on a set of data that includes "a session length and a shared secret." Therefore, applicant respectfully submits that Claim 5 is also in condition for allowance for these additional reasons.

Dependent Claims 8 and 21 add to the nonobviousness of applicant's invention by specifying that the first server-based application is an instant messaging server and specifying that the second server-based application is a Web server. The Office Action asserts that Kunzelman teaches "that the first server-based application is an instant messaging application that provides a different service than said second server-based application which is a Web application," and references Col. 1, lines 9-22 of Kunzelman in support of that proposition. (Office Action at page 4.) The Office Action incorrectly equates the use of server computers

capable of communicating using the HyperText Transfer Protocol ("HTTP") with allowing a user to access services offered by different applications based on a previous authorization. Those skilled in the art and others will recognize that HTTP is the application level protocol used to transmit markup code that embodies Web pages to a client-based browser application. However, other application level protocols may be used for implementing an instant messaging server. For example, the File Transfer Protocol ("FTP") or other application level protocol may be used for communicating using an instant messaging application. Therefore, applicant respectfully submits that Claim 8 is also in condition for allowance for these additional reasons.

Rejection of Claims 6 and 7 Under 35 U.S.C. § 103(a)

Claims 6 and 7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kunzelman as applied to Claim 1, and in further view of Wang. Since Claims 6 and 7 depend from Claim 1, the analysis applied to Claim 1 also applies to these claims. In addition, applicant submits that these dependent claims are allowable for additional reasons described below.

Dependent Claim 6 adds to the nonobviousness of applicant's invention the combination of (1) starting a persistence timer; (2) determining whether said persistence timer has reached a predefined value prior to receiving a response from said server-based application; and (3) in response to determining that said persistence timer has reached a predefined value prior to receiving a response from said second server-based application, deleting said authorization ticket, said session length and said hash value from said client computer." The Office Action asserts that Wang teaches these additional elements recited in Claim 6, stating that "Wang teaches that when a data packet (i.e., authentication ticket) is sent, a sequence variable is allocated and an acknowledgement timer (i.e., persistence timer) is set to prevent waiting indefinitely." (Office Action at page 6.) However, a system that prevents deadlocks (i.e., waiting indefinitely) as disclosed in Wang is not equivalent to the elements recited in Claim 6.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

More specifically, Claim 6 recites using a persistence timer to periodically check to determine if a predetermined amount of time has elapsed. This is not equivalent to using an acknowledgement timer to prevent deadlocks. Therefore, applicant respectfully submits that Claim 6 is also in condition for allowance for these additional reasons.

Dependent Claim 7 adds to the nonobviousness of applicant's invention the combination of "in response to determining that said persistence timer has not reached a predefined value prior to receiving a response from said second server-based application, receiving said response from said second server-based application and displaying said response at said client computer." The Office Action asserts that Wang teaches the additional elements recited in Claim 7. However, applicant is unable to find any reference in Wang to displaying the results of an authentication process. Instead, Wang is directed to a channel access protocol for implementing a wireless data network that does not involve interactions with a user. Therefore, applicant respectfully submits that Claim 7 is also in condition for allowance for these additional reasons.

Rejection of Claims 2-4, 10, and 12 Under 35 U.S.C. § 103(a)

Claims 2-4, 10, and 12 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kunzelman as applied to Claim 1 and in further view of Misra. Since Claims 2-4 depend, directly or indirectly, from Claim 1, and Claims 10 and 12 are computer apparatus and computer-readable medium claims with language that parallels Claim 1, the analysis applied to Claim 1 also applies to these claims. Therefore, applicant respectfully submits that Claims 2-4, 10, and 12 are in condition for allowance for the same reasons as Claim 1. In addition, applicant submits that these dependent claims are allowable for additional reasons described below.

Claim 2 recites a combination of steps "wherein said authorization ticket comprises a time stamp, and wherein determining a session length comprises subtracting said time stamp from an elapsed time counter to determine said session length." The Office Action takes Official

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Notice that "computing a session length by subtracting a timestamp from an elapsed time counter is old and well-known in the art." (Office action at page 8.) However, the Office Action does not show that the combination of steps recited in Claim 2 are well-known in the art. Namely, the Office Action does not show and Misra does not disclose including a timestamp in an authorization ticket that is transmitted between computers for the purpose of computing a session length. Simply stated, the claimed combination of determining a session length based on the value of an elapsed time counter is not well known in the art and not disclosed or suggested in Misra. Therefore, applicant respectfully submits that Claim 2 is also in condition for allowance for these additional reasons.

Dependent Claims 3 and 4 add to the nonobviousness of applicant's invention of "starting the elapsed time counter when said authorization ticket is received from said first server-based application." The Office Action asserts that Kunzelman teaches these additional elements recited Claims 3 and 4, and references Col. 4, Table 1, elements 3 and 4 of Kunzelman in support of that proposition. (Office Action at page 6.) The referenced sections of Kunzelman indicate that the time of session creation and expiration are included in a token that is returned a client computer "as part of the URL." Applicant submits that performing an action, namely, starting an elapsed time counter as recited in Claims 3 and 4 is not the same as including a set of data in a token that is returned to a client computer "as part of the URL." Therefore, applicant respectfully submits that Claims 3 and 4 are also in condition for allowance for these additional reasons.

Rejection of Claims 14-16, 18, and 20 Under 35 U.S.C. § 103(a)

Claims 14-16, 18, and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Kunzelman as applied to Claim 13 and in further view of Misra and Hershey. Since, Claims 14 and 16 depend, directly or indirectly, from Claim 13, and Claims 18 and 20 are computer apparatus and computer-readable medium claims that depend from Claim 13, the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

analysis applied to Claim 13 also applies to these claims. Therefore, applicant respectfully submits that Claims 14-16, 18, and 20 are in condition for allowance for the same reasons as Claim 13. In addition, applicant submits that the dependent claims are allowable for additional reasons described below.

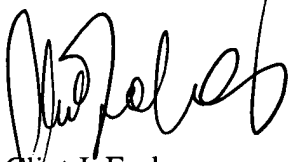
Dependent Claims 14-16 add to the nonobviousness of applicant's invention the element "in response to determining that the sum of said session line and said time stamp is within said preset threshold value, authorizing said client computer to access said second server-based application." The Office Action asserts that Hershey teaches these additional elements and cites Col. 7, lines 34-43, of Hershey in support of that proposition. Applicant submits that Hershey does not authorize client computers to access any server-based application. Instead, the system disclosed in Hershey determines if "the current message packet has expired" using a time stamp. (Hershey at Col. 7, lines 38-40.) If the message packet has not expired, then the message is rebroadcast. Applicant submits that rebroadcasting a message packet based on a time stamp is not equivalent to "authorizing said client computer to access said second server-based application." Therefore, applicant respectfully submits that Claims 14-16 are also in condition for allowance for these additional reasons.

CONCLUSION

In view of the foregoing claim amendments and remarks, applicant submits that all of the pending claims are in condition for allowance. Reconsideration and favorable action are requested. If the Examiner has any questions or comments concerning this matter, the Examiner is invited to contact applicant's undersigned attorney at the number provided below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS[PLLC]



Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first class mail with postage thereon fully prepaid and addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: January 27, 2006 Deborah L. Whitney

CJF:lal

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS[PLLC]
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100